REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application are obvious under the provisions of 35 U.S.C. § 103. The Applicants herein amend claims 1 and 15. Thus, the Applicants believe that all of these claims are now in allowable form.

I. REJECTION OF CLAIMS 1-8 AND 10-19 UNDER 35 U.S.C. § 103

A. Claims 1, 3-8, 11-15 and 17-19

The Examiner rejected claims 1, 3-8, 11-15 and 17-19 as being unpatentable over Talpade, et al. (U.S. Patent Publication No. 2004/0148520, published on July 29, 2004, hereinafter referred to as "Talpade") in view of Afek, et al. (U.S. Patent Publication No. 2002/0083175, published on June 27, 2002, hereinafter referred to as "Afek"). The Applicants respectfully traverse the rejection.

Talpade teaches mitigating denial of service attacks. Talpade teaches rerouting all traffic from all routers to a filter router when a denial of service attack is detected. (See Talpade, Abstract).

Afek teaches methods and apparatus for protecting against overload conditions on nodes of a distributed network. Afek teaches diverting traffic intended to a victim to one or more guardian nodes for filtering traffic when a denial of service attack is detected. (See Afek, Abstract; para. [0246] – [0265]).

The Examiner's attention is directed to the fact that Talpade and Afek, either alone or in any permissible combination, fail to teach or suggest a network or method comprising a router for injecting a routing instruction or a second IP address comprising a routing instruction having a same IP address as a first IP address, but with a higher preference value than the first IP address and having a community value such that a selected first number of edge routers direct VPN traffic addressed for said first IP address to said VPN application and a selected second number of edge routers direct VPN traffic addressed for said second IP address to said black-hole router, as positively claimed by the Applicants. Specifically, Applicants' independent claims 1, 8 and 15 positively recite:

1. An internet service provider (ISP) Virtual Private Network (VPN) network comprising:

a plurality of edge routers;

a plurality of core routers adapted to allow communication between said plurality of edge routers;

a VPN application in communication with a first one of said plurality of edge routers, said VPN application having a first IP address; and

a black-hole router in communication with said plurality of core routers, said black-hole router adapted to inject a second IP address into said ISP VPN network, said second IP address comprising:

a same IP address as the first IP address;

a higher preference value than said first IP address; and

a community value such that when said second IP address is injected, a selected first number of edge routers direct VPN traffic addressed for said first IP address to said VPN application and a selected second number of edge routers direct VPN traffic addressed for said second IP address to said black-hole router. (Emphasis added).

8. An internet service provider (ISP) network comprising:

a plurality of edge routers;

an application in direct or indirect electrical communication with a first one of said plurality of edge routers;

said application having a first IP address such that Virtual Private Network (VPN) traffic addressed for said first IP address and entering said ISP network at anyone of said plurality of edge routers, is routed to said application;

a black-hole router; and

a router adapted to inject an instruction into said ISP network, such that one or more select edge routers redirect VPN traffic, which is addressed to said first IP address, to said black-hole router, wherein said injected instruction comprises a routing instruction having a same IP address as said first IP address, but with a higher preference value than said first IP address and having a community value. (Emphasis added).

15. A method of managing a Distributed Denial of Service (DDoS) attack on an application within an internet service provider (ISP) network, said application having a first IP address, said method comprising:

injecting a Border Gateway Protocol (BGP) routing instruction into said ISP network when said DDoS attack is occurring, said BGP routing instruction comprising a second IP address having a same IP address as said first IP address, but with a higher preference value than said first IP address and having a community value;

redirecting, at one or more selected edge routers, VPN traffic addressed for said second IP address to a black-hole router; and

directing, at one or more other edge routers, VPN traffic addressed for said first IP address to said application that is experiencing said DDoS attack. (Emphasis added).

In one embodiment, the present invention provides a network or method comprising a router for injecting a routing instruction or a second IP address comprising a routing instruction having a same IP address as a first IP address, but with a higher preference value than the first IP address and having a community value such that a selected first number of edge routers direct VPN traffic addressed for said first IP address to said VPN application and a selected second number of edge routers direct VPN traffic addressed for said second IP address to said black-hole route. For example, the Applicants' invention may selectively re-route traffic of one or more edge routers by using preference and community values of an injected instruction or second IP address that is identical to a first address. (See e.g., Applicants' specification, page 11, line 16 – page 12, line 5).

Talpade and Afek fail to render obvious the Applicants' invention because Talpade and Afek fail to teach or suggest a network or method comprising a router for injecting a routing instruction or a second IP address comprising a routing instruction having a same IP address as a first IP address, but with a higher preference value than the first IP address and having a community value such that a selected first number of edge routers direct VPN traffic addressed for said first IP address to said VPN application and a selected second number of edge routers direct VPN traffic addressed for said second IP address to said black-hole route. First, the Applicants note that both Talpade and Afek teach away from the Applicants' invention. The Applicants' invention teaches that only a select number of edge routers (i.e. less than all or a subset of all the routers) are instructed to re-direct traffic to the black hole router, while the remaining routers continue to forward traffic to the VPN application. Thus, only some of the VPN traffic is diverted to the black hole router.

In stark contrast, both Talpade and Afek explicitly teach that all traffic is redirected either to the router filter or the guardian machines. Talpade teaches

"[t]he new routing information instructs the border and edge routers to reroute all DDoS and non-DDoS traffic directed at the customer network under attack to the filter router using the IP-in-IP tunnels. (See Talpade, para. [0009], emphasis added). Afek teaches "[u]pon receiving the alert of a possible attack on a victim all these border routers are set to forward all the traffic arriving from outside of the network (protected area) and whose destination IP address is the victim public IP address, to the guard machine which is placed next to them." (See Afek, para. [0257], emphasis added). As noted above, the Applicants' invention teaches that the injected routing instruction contains a second IP address that is the same as the first IP address, but having a higher preference value and a community value. In other words, all traffic is still forwarded to the system under attack. However, once it reaches the system under attack, only some of the traffic is diverted to the black hole router, while the remaining traffic is forwarded to the VPN application. In other words, unlike Talpade and Afek, the Applicants' invention only diverts a portion of the VPN traffic destined for the system under attack to the black hole router.

Moreover, the Examiner concedes that Talpade fails to teach or suggest this limitation in the Office Action. (See Office Action, p. 2, § 2). However, the Examiner asserts that Afek bridges the substantial gap left by Talpade. The Applicants respectfully disagree.

Afek fails to bridge the substantial gap left by Talpade because Afek also fails to teach or suggest a network or method comprising a router for injecting a routing instruction or a second IP address comprising a routing instruction having a same IP address as a first IP address, but with a higher preference value than the first IP address and having a community value such that a selected first number of edge routers direct VPN traffic addressed for said first IP address to said VPN application and a selected second number of edge routers direct VPN traffic addressed for said second IP address to said black-hole route. The Examiner continues to assert that Afek teaches the above limitation on paragraph [0257]. The Examiner's attention is directed to the fact that paragraph [0257] only teaches that redirecting all of the traffic to a guardian machine may

be accomplished by injecting an appropriate update. (See Afek, para. [0257]). However, paragraph [0257] is silent as to what kind of update is injected.

The Examiner's attention is directed to the fact that when Afek is read in its entirety, Afek clearly teaches that the injected update is a different IP address than the destination IP address of the victim. As previously noted, Afek teaches the use of two different IP addresses (i.e. a public IP address and a private IP address). (See Afek, para. [0255]). Afek specifically teaches that links that connect to either other networks or to external hosts and customer networks are permanently programmed to discard traffic destined to the server private IP address. (See Afek, para. [0256]). Moreover, neither the public nor the private IP address appears to be injected by any of the routers.

In stark contrast, the Applicants' invention teaches that a routing instruction or a second IP address having a same address as a first IP address is injected by a router. Thus, attack traffic may still be forwarded. However, the Applicants' invention teaches that the routing instruction or the second IP address has a higher preference value than the first IP address and a community value such that some routers selectively forward traffic to a black-hole router. Unlike the Applicants' invention, incoming traffic that has the private IP address taught by Afek is simply dropped. (See Afek, para. [0256]). The private IP address used by Afek is only for packet transfer between guard nodes and the victim. (See Afek, para. [0255]).

In addition, Afek fails to teach or suggest a second IP address having a community value. For example, in the Applicants' invention the community value may be determined by a router to select which routers will re-direct traffic. Thus, some routers may still be able to forward legitimate traffic to the recipient. Nowhere in Afek does it teach or suggest this characteristic of the public or private IP address. Moreover, paragraph [0248] only teaches that traffic is diverted to the guard nodes. (See Afek, para. [0248]). Notably, Afek does not teach or suggest that the traffic is diverted due to some parameter in the private or public IP addresses mentioned subsequent to paragraph [0248]. Rather, Afek teaches that traffic is diverted when an attack is detected. (See *Id.*).

The Examiner is reminded that the MPEP § 2141.02(VI) requires the Examiner to consider the prior art in its entirety. "A prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention". MPEP § 2141.02(VI), W.L. Gore & Associates, Inc., v. Garlock, Inc., 721 F.2d 1540, 220 USPQ 303 (Fed Cir. 1983), cert. denied, 469 U.S. 851 (1984). Thus, when the Examiner reads Afek in its entirety, the Applicants submit that the Examiner will find that the updating mechanism used by Afek is not the same as the updating mechanism used by the Applicants' invention. Specifically, Afek uses an update having a different IP address to divert all incoming traffic to the guardian router and the Applicants' invention uses an update having the same IP address, but with a higher preference value and a community value, such that only some of the incoming traffic is diverted to the black hole router. Thus, Talpade and Afek, alone or in any permissible combination, fail to render obvious Applicants' independent claims 1, 8 and 15.

In addition, dependent claims 3-7, 11-14 and 17-19 depend from independent claims 1, 8 and 15, respectively, and recite additional limitations. As such, and for the exact same reason set forth above, the Applicants submit that claims 3-7, 11-14 and 17-19 are also patentable over Talpade and Afek and respectfully request the rejection be withdrawn.

B. Claims 2, 10 and 16

The Examiner rejected claims 2, 10 and 16 as being unpatentable over Talpade in view of Afek and in further view of Yamauchi (U.S. Patent Publication No. 2002/0037010, published on March 28, 2002, hereinafter referred to as "Yamauchi"). The Applicants respectfully traverse the rejection.

The teachings of Talpade and Afek are discussed above. Yamauchi teaches a MPLS-VPN service network. The MPLS-VPN service network includes an interface identifying device. (See Yamauchi, Abstract).

The Examiner's attention is directed to the fact that Talpade, Afek and Yamauchi, alone or in any permissible combination, fail to disclose the network or method comprising a router for injecting a routing instruction or a second IP

address comprising a routing instruction having a same IP address as a first IP address, but with a higher preference value than the first IP address and having a community value such that a selected first number of edge routers direct VPN traffic addressed for said first IP address to said VPN application and a selected second number of edge routers direct VPN traffic addressed for said second IP address to said black-hole route, as positively claimed by the Applicants' independent claims 1, 8 and 15. (See *supra*). As discussed above, the alleged combination (as taught Talpade and Afek) simply does not teach or suggest the novel network or method comprising a router for injecting a routing instruction or a second IP address comprising a routing instruction having a same IP address as a first IP address, but with a higher preference value than the first IP address and having a community value such that a selected first number of edge routers direct VPN traffic addressed for said first IP address to said VPN application and a selected second number of edge routers direct VPN traffic addressed for said second IP address to said black-hole route.

Moreover, Yamauchi does not bridge the substantial gap left by Talpade and Afek because Yamauchi also fails to teach or suggest a network or method comprising a router for injecting a routing instruction or a second IP address comprising a routing instruction having a same IP address as a first IP address, but with a higher preference value than the first IP address and having a community value such that a selected first number of edge routers direct VPN traffic addressed for said first IP address to said VPN application and a selected second number of edge routers direct VPN traffic addressed for said second IP address to said black-hole route. Yamauchi only teaches a MPLS-VPN service network. (See Yamauchi, Abstract). Thus, for all of the above reasons, the Applicants respectfully contend that claims 1, 8 and 15 of the present invention are not made obvious by the combination of Talpade, Afek and Yamauchi.

Moreover, dependent claims 2, 10 and 16 depend from independent claims 1, 8 and 15, respectively, and recite additional limitations. As such, and for the exact same reason set forth above with regard to independent claims 1, 8 and 15 being patentable over Talpade, Afek and Yamauchi, the Applicants

submit that claims 2, 10 and 16 are also patentable over Talpade, Afek and Yamauchi. As such, the Applicants respectfully request the rejection be withdrawn.

CONCLUSION

Thus, the Applicants submit that all of these claims now fully satisfy the requirements of 35 U.S.C. § 103. Consequently, the Applicants believe that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the maintenance of the present final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 842-8110 x130 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully Submitted,



May 4, 2009

Wall & Tong, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 842-8110 x130